Vol 2 No 2, 2025 || E-ISSN 3032-6796 P-ISSSN 3032-4297

Journal of Law and Humanity Studies

Journal homepage:
https://journal.mediamandalika.com/index.php/jlhs

Limitations and Scope of the Government's Role in Law Number 1 of 2024 concerning Electronic Information and Transactions

Jimmy Simanjuntak
Faculty of Law, Universitas Kristen Indonesia, Indonesia
Email: jimmy.simanjuntak@uki.ac.id

KEYWORDS

Role of Government, General Principles of Good Governance, Digital Space, Legal Certainty.

ABSTRACT

The government has an important role in maintaining digital space. This certainly cannot be denied by anyone regarding the role of the government in supervising the actions of the community. However, the community must also be active in supervising the role of the government in digital media. This action is part of the participation of the community and government in managing digital space based on applicable national laws. The government in carrying out supervision is prohibited from limiting the space for community freedom in digital space. The government's authority in digital space must be supervised as it should be, so that threats to public order are maintained. Telematics law in Indonesia with its development continues to increase government authority in digital space so that through this, the community must create boundaries regarding government efforts in enforcing the law and government actions that exceed the limits of its authority in digital space.

1. Introduction

The digital space is different from the conventional space, as evidenced by the convergence of telematics law, which positions conventional law to be connected within the regulation of the digital space. The status of the digital space is different from conventional space, so its regulations must be crafted in such a way as to ensure legal certainty within the digital space. In the context of Indonesia's digitization, it does not directly grant freedom to the digital space, but there is government intervention in overseeing digital media.

The legal products regarding Information and Electronic Transactions have evolved, which can be summarized with the following legislative products:

1. Law of the Republic of Indonesia No. 11 of 2008 (Law on Electronic Information and Transactions 2008)
2. Law of the Republic of Indonesia No. 19 of 2016 (Law on Electronic Information and Transactions 2016)
3. Law of the Republic of Indonesia No. 1 of 2024 (Law on Electronic Information and Transactions)

This evolution has also changed the perspective on the role of the government within these laws. Through Law No. 11 of 2008, the government's role can be briefly explained in Article 40 of the Law as follows:

1. Article 40 of Law 11/2008:
   (1) The government facilitates the utilization of Information Technology and Electronic Transactions in accordance with the provisions of the legislation.
   (2) The government protects the public interest from any form of disruption caused by the misuse of Electronic Information and Electronic Transactions that disturb public order, in accordance with the provisions of the legislation.
   (3) The government establishes agencies or institutions that have strategic electronic data that must be protected.
   (4) The agencies or institutions referred to in paragraph (3) must create Electronic Documents and backup records and link them to a specific data center for data security purposes.
2. Article 40 of Law 19/2016:
   (1) The government facilitates the utilization of Information Technology and Electronic Transactions in accordance with the provisions of the legislation.
   (2) The government protects the public interest from any form of disruption caused by the misuse of Electronic Information and Electronic Transactions that disturb public order, in accordance with the provisions of the legislation.

(2a) The government must prevent the dissemination and use of Electronic Information and/or Electronic Documents containing prohibited content according to the legislation. (2b) In carrying out the prevention as referred to in paragraph (2a), the government is authorized to disconnect access and/or instruct Electronic System Providers to disconnect access to Electronic Information and/or Electronic Documents that contain unlawful content.
(3) The government establishes agencies or institutions that have strategic electronic data that must be protected.
(4) The agencies or institutions referred to in paragraph (3) must create Electronic Documents and backup records and link them to a specific data center for data security purposes.
(5) Other agencies or institutions not regulated in paragraph (3) must create Electronic Documents and backup records in accordance with the data protection needs they possess.
(6) Further provisions regarding the government's role as referred to in paragraph (1), (2), (2a), (2b), and (3) are regulated in government regulations.

3. Article 40 of Law 1/2024:
(1) The government facilitates the utilization of Information Technology and Electronic Transactions in accordance with the provisions of the legislation.
(2) The government protects the public interest from any form of disruption caused by the misuse of Electronic Information and Electronic Transactions that disturb public order, in accordance with the provisions of the legislation. (2a) The government must prevent the dissemination and use of Electronic Information and/or Electronic Documents containing prohibited content according to the legislation. (2b) In carrying out the prevention as referred to in paragraph (2a), the government is authorized to disconnect access and/or instruct Electronic System Providers to disconnect access to Electronic Information and/or Electronic Documents that contain unlawful content. (2c) The instruction to the Electronic System Provider as referred to in paragraph (2b) includes disconnecting access and/or moderating content independently for Electronic Information and/or Electronic Documents containing pornography, gambling, or other prohibited content according to the legislation, as long as it is technically feasible. (2d) In carrying out the prevention as referred to in paragraph (2a), the government is authorized to instruct the Electronic System Providers to moderate content for Electronic Information and/or Electronic Documents that pose a threat to individual or public safety or health.
(3) The government establishes agencies or institutions that have strategic electronic data that must be protected.
(4) The agencies or institutions referred to in paragraph (3) must create Electronic Documents and backup records and link them to a specific data center for data security purposes.
(5) Other agencies or institutions not regulated in paragraph (3) must create Electronic Documents and backup records in accordance with the data protection needs they possess.
(6) Further provisions regarding the government's role as referred to in paragraphs (1), (2), (2a), (2b), (2c), (2d), and (3) are regulated in government regulations.

As previously explained, the development of the government's role in the provisions of Article 40 of the Electronic Information and Transactions Law has continued to change in each legislative amendment, and even in the most recent change, Article 40A of the Law on Electronic Information and Transactions has been added.

In the first revision, the 2016 Law on Electronic Information and Transactions, in Article 40 paragraph (2a), there is already a form of repressive authority, as seen in the phrase "The government is obligated to prevent," followed by Article 40 paragraph (2b), which states "The government has the authority to disconnect access and/or instruct Electronic System Providers to disconnect access." This stance could potentially contradict the freedom inherent in the existing legislation. Then, in Article 40 paragraph (2c) of the 2016 Law, there is the phrase "in the form of disconnecting access and/or independently moderating content for Electronic Information and/or Electronic Documents containing pornography, gambling, or other content," which refers to Article 40 paragraph (2b), but the phrase "or other content" does not provide clear legal certainty regarding its boundaries.

This legal uncertainty burdens society, as the use of the digital space becomes more problematic if the government is not given clear limits by law. If we look at Article 40 paragraph (2b) of the Law, the phrase "containing unlawful content" must also be clarified regarding the boundaries of its legal application. It is essential to underline that the digital space also has its own set of rules known as "Terms and Conditions" (TNC), which apply to all users without the intervention of each country's laws.

Therefore, the problem regarding the government's role in the Law on Electronic Information and Transactions lies in Article 40 paragraph (2c) with the phrase "or other content"

and in Article 40 paragraph (2b) with the phrase "containing unlawful content," which lack a solid foundation of legal certainty and create a conflict with the TNCs that apply in a digital space. As an introduction, it is also necessary to consider the principles that apply in telematics law, namely:

1. Subjective territoriality: From this perspective, the law applies based on where cybercrimes occur, and their legal resolution is carried out in another country.
2. Objective territoriality: From this perspective, the law applies based on where the primary consequences of the crime occur and cause significant damage to the concerned country.
3. Nationality: In this perspective, the state has jurisdiction to determine the law based on the perpetrator's nationality.
4. Passive nationality: This emphasizes jurisdiction based on the nationality of the victim.
5. Protective principle: In this perspective, the law is based on a country's desire to protect its interests from crimes committed outside its borders, typically when the victim is the state or government.
6. Universality: This principle deserves special attention regarding the handling of cybercrime cases. It is also referred to as "universal interest jurisdiction."

2. Result and Discussion

Government Limitations According to the General Principles of Good Governance (AUPB) Linked to Abuse of Power Concerning the ITE Law

Through the concept of the General Principles of Good Governance (AUPB) as the foundation for discussion, it is necessary to first elaborate on AUPB in Article 10 of Law No. 30 of 2014 on Government Administration (UU AP), which includes legal certainty, benefits, impartiality, accuracy, non-abuse of authority, transparency, public interest, and good service. With these principles in mind, the government's power in Article 40 of the ITE Law needs to be interpreted in accordance with the applicable AUPB provisions. First and foremost, the government, when examining actions that "contain unlawful content," must consider the AUPB, particularly the principle of legal certainty, which ensures that:

Legal certainty is meant to respect the legal rights of individuals based on a policy. Through this, the government, in exercising its authority under Article 40 of the ITE Law, must consider the rights of those sanctioned in accordance with the applicable laws.

The correlation with Indonesia is that the state is governed by the rule of law, and the authority of the government is explained by Dicey as follows:

1. Supremacy of law, meaning that the highest power in the state is the law;
2. Equality before the law, meaning every person is equal under the law;
3. The constitution is not the source of human rights (HAM), but human rights, if placed in the constitution, only affirm that these rights must be protected.

It is clear from this that the government has legal limitations in exercising its power. This is certainly correlated with the increasing power of the government in each amendment to the law concerning Information and Electronic Transactions.

To limit the scope of government subjects in the ITE Law, Article 1 point 23 of the ITE Law defines "the government as the Minister or other officials appointed by the President," as stated in Article 1 point 25 of the Government Administration Law, which reads, "The Minister is the minister who handles government affairs in the field of state apparatus utilization." In AUPB, it is written that abuse of power (detournement de pouvoir) is prohibited and can be interpreted as "not mixing authority, where government officials have powers already defined by regulations (both in terms of material, territory, and time) to take legal actions to serve and regulate citizens."

The imposition of administrative sanctions in Article 40 of the ITE Law is outlined in Article 40A of the ITE Law (the second amendment to the ITE Law 2008), which states:

1. The government is responsible for encouraging the creation of a fair, accountable, secure, and innovative digital ecosystem.
2. To implement the responsibilities as referred to in paragraph (1), the government has the authority to order Electronic System Providers to adjust their electronic systems and/or take specific actions.
3. Electronic System Providers must carry out the order referred to in paragraph (2).
4. If Electronic System Providers violate the obligations referred to in paragraph (3), they will be subjected to administrative sanctions.
5. Administrative sanctions referred to in paragraph (4) can include:
   a. Written warning;
   b. Administrative fines;
   c. Temporary suspension; and/or
   d. Access termination.
6. Further provisions regarding the government's responsibilities as referred to in paragraph (1), the government's authority as referred to in paragraph (2), the obligations of Electronic System Providers as referred to in paragraph (3), and the imposition of administrative sanctions as referred to in paragraphs (4) and (5) are regulated in government regulations.

Provisions in Article 40 and Article 40A of the ITE Law are part of the government's role as a public servant and cannot be separated from AUPB. Therefore, this must be under public supervision. This is because the imposition of administrative sanctions is part of **beschikking**, as "almost all government organs have the authority to issue determinations or decisions," which are limited in that "determinations that meet both material and formal requirements are deemed valid by law and can be accepted as part of the legal order."

In the case of Article 40 of the ITE Law, the government, in imposing sanctions, must meet the material conditions stipulated in Article 40 paragraphs (2a) and (2b) of the ITE Law. This is part of the government's authority to maintain public order and perform its public service functions. However, the real reason for the existence of Article 40 paragraphs (2c) and (2d) is that the government has the authority to independently moderate "other content as referred to in the regulations" and to order the electronic system providers to moderate "electronic documents that contain content dangerous to the safety of individuals or public health." This should be better understood in the historical context of the ITE Law from its creation until now. Historically, the ITE Law was challenged in the Constitutional Court in Decision No. 78/PUU-XVII/2019, which determined that Article 27 paragraph (3) of the ITE Law was not unconstitutional. However, this provision was removed in the latest version of the ITE Law. The removal of Article 27 paragraph (3) of the ITE Law in the update was not arbitrary. It included the addition of Article 40 paragraphs (2c) and (2d) and Article 40A. The government's increased authority in the digital space raises questions about the function of these provisions within the digital legal system.

The Rights of the Public to Seek Legal Recourse and the Role of Society Acknowledged by Law

In carrying out its functions within Indonesia's legal system, society must comply with the applicable laws. In the case of administrative sanctions being imposed on a party, legal recourse is available. The legal action available for the public to challenge administrative sanctions deemed unjust is to file a lawsuit with the State Administrative Court (PTUN), where the public can challenge:
a. A State Administrative Decision that contradicts the applicable laws and regulations;
b. A State administrative body or official that, when issuing a decision, has used its authority for purposes other than those for which the authority was granted;
c. A State administrative body or official that, when issuing a decision, failed to consider all relevant interests involved.
This is further supported by the following principles in PTUN:

1. Presumption of Lawfulness (Rechtmatig), meaning any action by the authorities is presumed lawful unless proven otherwise.
2. Free Proof Principle, where the judge determines the burden of proof, the type of evidence required (documents, expert testimony, witness statements, party admissions, judicial knowledge), and at least two pieces of evidence are needed for proof to be accepted.
3. Active Role of Judges (Dominus Litis), which aims to balance the unequal positions of the parties.
4. Binding Legal Decision (Erga Omnes), meaning decisions made in public law disputes are binding on all, not just the parties involved.

Based on the aforementioned principles of PTUN, the government, when exercising its sanctioning authority, is subject to legal recourse for those subjected to sanctions who feel they are unjust. PTUN is closely related to good governance, as it involves:

1. Guaranteeing security for all persons and society;
2. Managing an effective framework for the public sector, the private sector, and civil society;
3. Promoting economic, social, and other objectives according to the will of the people.

In addition, society is also given a role under the ITE Law, which grants legal legitimacy for the role of society. Public participation under the ITE Law is regulated in Article 41 of the ITE Law, which limits society's role. The law does not include significant changes regarding the role of society. Article 41 of the ITE Law reads:

1. The public can contribute to enhancing the utilization of Information Technology through the use and management of Electronic Systems and Electronic Transactions in accordance with the provisions of this Law.
2. The role of the public as referred to in paragraph (1) can be carried out through institutions established by the public.
3. The institution referred to in paragraph (2) may serve consultation and mediation functions.

Thus, in exercising its powers, the government must be limited, and there must be a balance between the government's authority and the applicable laws. PTUN serves as a basis for challenging the abuse of power by the government, as part of the public's right to access legal certainty.

3. Conclusion

The conclusion of this discussion shows that the development of legislation regarding Electronic Information and Transactions, especially in terms of the role of the government, has undergone significant changes

from the 2008 ITE Law to the 2024 ITE Law. This change shows the addition of government authority in regulating and supervising the digital space, especially through the provisions in Article 40 and Article 40A of the ITE Law which give the government the authority to decide on access and order electronic system organizers to moderate content. However, this authority also creates the potential for legal uncertainty, especially related to the phrases "having unlawful content" and "other content," which require clearer definitions so as not to excessively limit freedom in the digital space. In addition, it is necessary to ensure that the government's role in the digital space remains in accordance with the general principles of good governance, including maintaining legal certainty and not abusing authority.

On the other hand, although the government is given quite a lot of authority in regulating the digital space, the public also has the right to take legal action through the State Administrative Court (PTUN) if they feel aggrieved by decisions issued by the government. This reflects the importance of a balance between government authority and the rights of the public in the Indonesian legal system, which must be regulated clearly and transparently. The community, although its role is limited in the ITE Law, can still participate in improving the use of information technology through institutions formed by the community. Therefore, the role of supervision by the community and the courts is very important to ensure that the implementation of government authority in the digital space remains based on the principle of good governance and does not violate individual rights.

4. References

Dian Aries Mujiburohman, 2022, Hukum Acara Peradilan Tata Usaha Negara, STPN Press, Yogyakarta.

Haposan Siallagan, Kasman Siburian, dan Fernando Z. Tampubolon, 2019, Hukum Acara Peradilan Tata Usaha Negara, Lembaga Pemberdayaan Media dan Komunikasi, Medan.

Imam Mahdi dan H. Iskandar Zulkarnain Oktaria, Hukum Administrasi Negara, 2013, IPB Press, Bogor.

Muhammad Zainul Arifin dan Firman Muntaqo, "Penerapan Prinsip Detournement De Pouvoir Terhadap Tindakan Pejabat BUMN Yang Mengakibatkan Kerugian Negara Menurut Undang-Undang Nomor 17 Tahun 2003 Tentang Keuangan Negara", 2018, Nurani, 18 (2).

Nurul Hidayah Tumadi, 2023, "Keputusan Tata Usaha Negara (Beschikking)", Siyasah: Jurnal Hukum Tata Negara, 6(II).

S.F. Marbun, et. al., Dimensi-dimensi Pemikiran Hukum Administrasi Negara, 2001, UII Press, Yogyakarta.

Sahat Maruli T. Situmeang, Cyber Law, 2020, Cakra, Bandung.